AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS

1. (Previously Presented) A system for executing a software application comprising a plurality of hardware independent bytecodes, the system comprising:

a computing system data generates bytecodes;

a virtual machine, remote to the computing system, comprising means for receiving a plurality of authenticated bytecodes from said computing system, and means for executing said plurality of authenticated bytecodes;

means for testing said bytecodes against a set of predetermined criteria; and

means for securely distributing said testing means between said virtual machine and said computing system so that bytecode testing completed by the computing system is authenticated by the virtual machine prior to the execution of the authenticated bytecodes by said virtual machine.

2-23 (Canceled)

24. (New) A method for controlling a device having an external port and a microcontroller configured to run a virtual machine, the method comprising:

receiving through the port, code including virtual machine code for use by the virtual machine;

determining whether the code is authentic in response to an indicator of authenticity provided within the code; and

if the code is determined to be authentic, then

omitting processing of particular code provided within the received code according to at least some of a predetermined set of processes, and

executing the particular code, if the received code is determined to be authentic.

25. (New) The method of claim 24, further comprising verifying that the particular code conforms to at least one other of the predetermined set of criteria, if the received code is determined to be authentic.

26. (New) The method of claim 24 wherein the particular code comprises bytecode.

27. (New) An apparatus for controlling a device having an external port and a microcontroller configured to run a virtual machine, the apparatus comprising:

means for receiving through the port, code including virtual machine code for use by the virtual machine;

means for determining whether the code is authentic in response to an indicator of authenticity provided within the code; and

means for, if the code is determined to be authentic,

omitting processing of particular code provided within the received code according to at least some of a predetermined set of processes, and

executing the particular code, if the received code is determined to be authentic.

28. (New) The apparatus of claim 27, further comprising means for verifying that the particular code conforms to at least one other of the predetermined set of criteria, if the received code is determined to be authentic.

29. (New) The apparatus of claim 27 wherein the particular code comprises bytecode.

30. (New) An apparatus for programming a device having a microcontroller configured to execute a virtual machine and a port to a communications link from a remote computer connected to the communications link, the apparatus comprising:

means for verifying at said remote computer that particular virtual machine code for use by said virtual machine conforms to at least some of a predetermined set of criteria;

means for, if said particular virtual machine code passes said verifying,

generating at least one indicator of authenticity, and

sending code including said particular virtual machine code and said at least one indicator of authenticity from said remote computer to said device over said communications link;

means for receiving said code through said port at said device;

means for determining at the device whether said code is authentic in response to the at least one indicator of authenticity; and

means for, if said code is determined to be authentic,

omitting verification that said particular virtual machine code conforms to said at least same of the predetermined set of criteria, and

operating the virtual machine according to said particular virtual machine code.

31. (New) The apparatus of claim 30 wherein said device comprises a small footprint device.

32. (New) The apparatus of claim 30 wherein said device comprises a portable product.

33. (New) The apparatus of claim 30 wherein said device comprises a tamper-resistant package.

34. (New) The apparatus of claim 30 wherein said virtual machine code comprises bytecode.

35. (New) The apparatus of claim 30 wherein said at least some of the predetermined set of criteria comprises substantially all of said predetermined set of criteria.

36. (New) The apparatus of claim 30 wherein said at least one indicator of authenticity comprises an indication that said code is from a trusted source and an indication that said particular virtual machine code has not been corrupted since being sent by said trusted source.

37. (New) The apparatus of claim 30, further comprising means for, if said code is determined to be authentic, verifying said particular virtual machine code conforms to at least one other of said predetermined set of criteria.

38. (New) The apparatus of claim 30 wherein said means for determining whether said code is authentic is performed by said virtual machine.

39. (New) The apparatus of claim 30, further comprising means for, if said code is determined to be not authentic, operating said virtual machine according to said particular code.

40. (New) A memory for storing data for access by an application program being executed on a data processing system, comprising:

a data structure stored in said memory, said data structure including information used by said program to control a device having an external port and a microcontroller configured to execute a virtual machine, said data structure comprising a proof of authenticity and code received through the port, said code including virtual machine code for use by the virtual machine, said proof of authenticity for determining whether to omit processing of particular code provided within the received code according to at least some of a predetermined set of processes prior to executing the particular code.

41. (New) The memory of claim 40 wherein said proof of authenticity comprises a hash value.

42. (New) The memory of claim 40 wherein said proof of authenticity comprises a message authentication code using a block-cipher algorithm.

43. (New) The memory of claim 40 wherein said proof of authenticity comprises a digital signature using an symmetric cyrptographic algorithm.

44. (New) A computer program product for a programmable device having a microcontroller and an external port, the computer program product comprising:

a memory medium;

instructions, stored on the memory medium, to cause the microcontroller to

receive an authenticated bytecode by a virtual machine, said authenticated bytecode being previously compared against a predetermined set of criteria and having a proof of authenticity;

determinine whether said authenticated bytecode is corrupted based at least in part on said proof of authenticity; and

execute said bytecode.

45. (New) The computer program product of claim 44, said instructions further causing said microcontroller to, at run-time, check said authenticated bytecode for memory access errors.

46. (New) The computer program product of claim 44, said instructions further causing said microcontroller to, at run-time, generate a proof of authenticity, and compare the generated proof of authenticity against the proof of authenticity attached to the received bytecode.

47. (New) The computer program product of claim 44, said instructions further causing said microcontroller to, at run-time, store authenticated bytecodes in a non-volatile manner so that the authenticated bytecodes are not repeatedly communicated with the virtual machine.

48. (New) A method for executing a software application comprising a plurality of hardware independent bytecodes, the method comprising:

a computing system generating bytecodes;

a virtual machine, remote to the computing system,

receiving a plurality of authenticated bytecodes from said computing system, and

executing said plurality of authenticated bytecodes;

testing said bytecodes against a set of predetermined criteria, said testing securely distributed between said virtual machine and said computing system so that bytecode testing completed by the computing system is authenticated by the virtual machine prior to the execution of the authenticated bytecodes by said virtual machine.

49. The method of claim 48, said remote computing system determining that the bytecodes comply with a predetermined set of criteria to generate verified bytecodes, and generating a proof of authenticity attached to said verified bytecodes to generate authenticated bytecodes so that the authenticated bytecodes are tamper-resistant.

50. (New) The method of claim 49, said virtual machine determining whether the authenticated bytecodes are corrupted, comprising generating a proof of authenticity based on the received bytecodes, and comparing said generated proof of authenticity against said authenticated bytecodes.

51. (New) The method of claim 49, said virtual machine performing limited run-time testing of said authenticated bytecodes.

52. (New) The method of claim 49, said performing further comprising testing the memory access of said authenticated bytecodes.

53. (New) The method of claim 49, said virtual machine storing authenticated bytecodes in a non-volatile manner so that the authenticated bytecodes are not repeatedly communicated with the virtual machine.

54. (New) A method for executing a software application comprising a plurality of bytecodes, the method comprising:

a computer system

verifying that a bytecode conforms to a predetermined set of criteria to generate a verified bytecode, and

generating an authenticated bytecode from said verified bytecode; and

a virtual machine, remote from said computer system,

receiving said authenticated bytecodes,

determining whether the authenticated bytecodes are corrupted, and

executing said authenticated bytecodes if said authenticated bytecodes are not corrupted.

55. (New) The method of claim 54, said virtual machine performing limited run-time testing of said received bytecodes.

56. (New) The method of claim 54, said computing system generating a proof of authenticity and attaching said proof of authenticity to said bytecodes.

57. (New) The method of claim 55, said virtual machine generating a proof of authenticity and comparing said generated proof of authenticity against said received proof of authenticity to determine whether said received bytecode is corrupted.